The Center for Collaborative Systems for Security, Safety, and Regional Resilience

AT THE UNIVERSITY OF WASHINGTON

Information Security Guide

August 15, 2015

CENTER FOR COLLABORATIVE SYSTEMS FOR SECURITY, SAFETY & REGIONAL RESILIENCE

UNIVERSITY of WASHINGTON

Controlled Unclassified Information (CUI) Guidance

Issued and Approved by:

Dr. Mark Haselkorn, PhD. Director of CoSSaR

August 15, 2015

Date

Table 1: Version Control		
Version	**Change**	**Effective Date**
Version 1.0	Initial Version	8-15-2015

Table 2: Table of Changes				
Version #	Date	Section	Paragraph	Description

Table of Contents

List of Tables

1 GENERAL

1.1 PURPOSE

This Information Security Guide is issued for the purpose of identifying specific topics of information associated with projects under the Center for Collaborative, Safety, Security, and Regional Resilience (CoSSaR) that meet the standards and criteria for special handling and protection in accordance with Executive Order 13556, “Controlled Unclassified Information” (CUI). The document also provides guidance on handling sensitive information that requires protection against unauthorized disclosure, including information designated “Sensitive But Unclassified” (SBU) under current control programs, which will ultimately be transitioned to protect information under the new CUI regime.

This guide provides direction for identifying and properly handling the three categories of CUI/SBU information most likely to be encountered by the CoSSaR community:

- “For Official Use Only” (FOUO) (See Section 5)
- “Law Enforcement Sensitive” (LES) (See Section 6)
- “Sensitive Security Information” (SSI) (See Section 7)

All CoSSaR project information designated or determined to be CUI/SBU must be processed according to the requirements of this Information Security Guide. However, the vast majority of the information gathered, processed, analyzed, and produced in CoSSaR activities will be “Unclassified” information without the need for special handling. Unclassified information which is not designated CUI/SBU by the originator ***and*** which does not meet the criteria for CUI/SBU set forth in this Information Security Guide and reference documents in Section 1.2 does not require special handling or safeguarding.

This guide does not address national security classified information deemed Confidential, Secret, or Top Secret as set forth in Executive Order 13526.

1.2 AUTHORITY

This guide is approved by the Director of the Center for Collaborative, Safety, Security, and Regional Resilience at the University of Washington. It is issued to provide guidance to Federally directed CoSSaR activities in accordance with Executive Order 13556, Department of Homeland Security Management Directive Numbers 11042.1 and 11056.1, Department of Defense Manual Number 5200.01 (Volume 4), 49 CFR 1520.5, and University of Washington security directives.

1.3 SCOPE AND APPLICABILITY

This document provides security guidance for the use of CUI/SBU information associated with the CoSSaR program. This guide and reference authorities (listed in Section 1.2) shall be cited as the basis for recognizing, categorizing, marking, handling, processing, transmitting, and disseminating of CUI/SBU and materials. If a conflict exists between this guide and reference authorities, the reference authority takes precedence.

1.4 EFFECTIVE DATE AND IMPLEMENTATION

This guide is effective immediately upon release.

1.5 OFFICE OF PRIMARY RESPONSIBILITY

The Office of Primary Responsibility (OPR) for this guide is:

Program Manager
Center for Collaborative, Safety, Security, and Regional Resilience (CoSSaR)
310 Sieg Hall, Box 352315
University of Washington
Seattle, WA 98195
Phone: (206) 543-4640 Fax: (206) 543-8858 E-Mail: CoSSaR@uw.edu

The office of secondary responsibility for this guide is:

University Facility Security Officer
1013 NE 40th St., Box 355640
Seattle, WA 98105
Phone: (206) 543-1315 Fax: (206) 543-1732 E-Mail: uwfso@uw.edu

2 POLICY

2.1 GENERAL

One goal of CoSSaR is to produce relevant analytic products for Puget Sound area stakeholders that may be disseminated to the widest audience possible at the uncontrolled UNCLASSIFIED level. In the conduct of their work, CoSSaR researchers may, however, be given CUI/SBU information - or they may create it by compilation. To properly control information, it is essential for researchers to recognize CUI/SBU information.

When gathering information, it is ***required*** that CoSSaR researchers document when the information they receive is CUI/SBU information. All information marked as CUI/SBU by any Federal agency shall be marked and handled in accordance with this Information Security Guide within the CoSSaR project. It is the responsibility of each CoSSaR researcher to ask if information gathered in verbal interviews is either uncontrolled or CUI/SBU information.

Department of Homeland Security (DHS) Management Directive 11042.1 states “Any DHS employee, detailee, or contractor, can mark information falling within one or more of the categories as FOUO.” Therefore, acting as grantees or contractors to DHS, CoSSaR researchers may designate information falling into the categories below as “FOUO” to maintain protection of the information. Additionally, “DHS Officials occupying supervisory or managerial positions are authorized to designate other information, not listed and originating under their jurisdiction, as FOUO.”

If CoSSaR personnel believe that information meets the criteria for CUI/SBU information, the material should be sent to the sponsor team via DHS using approved CUI/SBU information transmission methods (see section 4.3) for final determination. In the interim, the material shall be protected as if it were CUI/SBU information until a final determination is made by DHS.

2.2 REASON FOR CONTROL

Most unclassified information encountered and produced during the conduct of research under the CoSSaR project will not be subject to special controls. However, certain categories of unclassified information are exempt from public release under the Federal Freedom of Information Act, the Privacy Act, and the US Code of Federal Regulations (CFR). This information is designated CUI/SBU information, and must be protected from unauthorized public release. (For more information on the details of the regulatory authority, see Sections 5, 6, and 7).

2.3 CONTROL BY COMPILATION

Analysis and compilation of uncontrolled unclassified information is normally not subject to the restrictions associated with CUI/SBU information. However, in certain circumstances, information that would otherwise be uncontrolled may become CUI/SBU information when combined or associated with other unclassified information, if the compiled information reveals an additional association or relationship, not otherwise evident by the individual items of information that meets the standard and criteria for CUI/SBU information. Under such circumstances, it is the additional association or relationship revealed by the combination or compilation of information that is CUI/SBU, not the individual items of information.

3 RELEASE OF INFORMATION

3.1 PUBLIC RELEASE

This guide is designated UNCLASSIFIED and subject to public release under the Federal Freedom of Information Act and Washington RCW Chapter 42.56 Public Records Act.

3.2 CONTROLLED UNCLASSIFIED INFORMATION

Executive Order 13556 "Controlled Unclassified Information" established the CUI program, which is a system that standardizes and simplifies the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies. Although President Obama signed Executive Order 13556 in 2009, many Federal agencies have yet to complete the transition to the CUI standard. As a result, much of the guidance for the previous “Sensitive But Unclassified” (SBU) regime remains in place.

This guide applies to certain types of CUI/SBU information for which Executive Branch agencies require applications of controls and protective measures for a variety of reasons. FOUO and LES are designations applied by DHS to CUI/SBU information, which may be exempt from mandatory release to the public under Section 552 of Title 5, U.S.C., “Freedom of Information Act (FOIA)” or “The Privacy Act”. SSI is the designation applied by DHS to CUI/SBU information obtained or developed in the conduct of security activities as defined in 49 C.F.R. Section 1520.5.

4 INFORMATION HANDLING

4.1 GENERAL HANDLING REQUIREMENTS

1. No security clearance is needed for access to CUI/SBU information; however, the recipient must have a ‘need to know’ the information.

2. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. CUI/SBU information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the materials shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items. CUI/SBU information should not be stored with classified information unless there is a correlation.

a. When removed from an authorized storage location and persons without a need-to-know are present, or where casual observation would reveal CUI/SBU information to unauthorized persons, a “FOR OFFICIAL USE ONLY” or “Sensitive Security Information” cover sheet will be used to prevent unauthorized or inadvertent disclosure. (For further information on cover sheets see Sections 4.2.2, 4.2.3, and 4.2.4.)

b. When forwarding CUI/SBU information, a FOUO or SSI cover sheet should be placed on top of the transmittal letter, memorandum, or document.

3. Unauthorized disclosure of CUI/SBU information doesn't constitute a security violation, but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of CUI/SBU information protected by the Privacy Act may result in criminal sanctions.

4. To obtain further guidance regarding For Official Use Only (FOUO) and Law Enforcement Sensitive (LES) refer to DHS Management Directive Number 11042.1.

5. To obtain further guidance regarding the handling of Sensitive Security Information (SSI) refer to DHS Management Directive Number 11056.1.

4.2 DOCUMENT MARKING

4.2.1 UNCLASSIFIED (U)

Unclassified refers to information that requires no security protection and can be released to individuals without restrictions. To identify unclassified information in a title, heading, paragraph, or bullet, precede it with a portion marking (abbreviated classifications listed before each paragraph) of "(U)". If a document contains uncontrolled unclassified material only, annotate "UNCLASSIFIED" in the header and footer, or do not place any classification markings on the document.

4.2.2 FOR OFFICIAL USE ONLY (FOUO)

To identify unclassified information, designate it with an "FOUO" caveat in a title, heading, paragraph, or bullet, precede the portion with "(U//FOUO)". If a document contains both "(U)" and "(U//FOUO)", the overall classification of the document is "UNCLASSIFIED//FOR OFFICIAL USE ONLY," as annotated in the header and footer.

Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. At a minimum, prominently mark on the bottom of each page "FOR OFFICIAL USE ONLY." Materials containing specific types of FOUO information may be further marked with an applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE", in order to alert the reader of the type of information conveyed. (See Section 4.2.3.) Additional access and dissemination restrictions may also be cited as the situation warrants.

The cover sheet of each document containing FOUO should be marked with the following warning:

(U) WARNING: This document is UNCLASSIFIED // FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or

other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

4.2.3 LAW ENFORCEMENT SENSITIVE (LES)

In unclassified documents containing LES information, the phrase “Law Enforcement Sensitive” shall accompany the phrase “FOR OFFICIAL USE ONLY” at the bottom of the outside of the front cover, the title page (if there is one), and the outside of the back cover (if there is one). Each page containing FOUO-LES information shall be marked “FOR OFFICIAL USE ONLY Law Enforcement Sensitive” at the bottom.

Portions of unclassified documents that contain FOUO-LES information shall be marked with the parenthetical notation “(FOUO-LES)” at the beginning of the portion. If an unclassified portion of a classified document contains FOUO-LES information, the portion marking (U//FOUO-LES) shall be used.

The cover sheet of each document containing LES should be marked with the following warning:

(U) WARNING: LAW ENFORCEMENT SENSITIVE. The information in this document marked FOUO-LES is the property of the Department of Homeland Security and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior DHS authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the FOUO-LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked FOUO-LES on a website or unclassified network.

4.2.4 SENSITIVE SECURITY INFORMATION (SSI)

To identify unclassified information with an “SSI” caveat in a title, heading, paragraph, or bullet, precede the portion with “(U//SSI)”. If a document contains “(U)”, “U//FOUO”, “(U//LES)”, and “(U//SSI)”, the overall classification of the document is “UNCLASSIFIED// LAW ENFORCEMENT SENSITIVE and SENSITIVE SECURITY INFORMATION”.

Individual paragraphs and sections properly marked as “Unclassified” or “(U)” may be shared freely, but other information properly marked as FOUO, LES, or SSI within a document can only be shared with authorized recipients who have a valid “need-to-know”.

The cover sheet of each document containing SSI should be marked with the following warning:

> *(U) WARNING: This record contains SENSITIVE SECURITY INFORMATION that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.*

4.2.5 ORIGINATION INFORMATION

Designator or originator information & markings, downgrading instructions, & date/event markings are not required on FOUO, LES, or SSI documents.

4.2.6 REMOVAL OF CUI MARKINGS AND DESIGNATION

Removal of CUI/SBU information markings can only be accomplished by the originator or other competent authority. ***DO NOT*** remove any CUI/SBU information markings

without written authorization from DHS, NAVSEA Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I), or the originator.

4.3 TRANSMISSION OF CUI/SBU INFORMATION

4.3.1 MAIL

Controlled Unclassified Information may be mailed via First Class Mail with the U.S. Postal Service, or an authorized commercial delivery service such as DHL or Federal Express.

a. SSI shall be mailed in a manner that offers reasonable protection of the sent materials and sealed in such a manner as to prevent inadvertent opening and show evidence of tampering.

b. SSI may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access (e.g., sealed envelope).

4.3.2 VOICE, DATA, AND FAX

Electronic transmission of CUI/SBU information (voice, data, or facsimile) should be by approved secure communications systems *whenever practical*.

a. Unless otherwise restricted by the originator, CUI/SBU information may be sent via non-secure fax. Where a non-secure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end.

4.3.3 ENCRYPTION

CUI/SBU information transmitted over email should be protected by encryption, such as the use of password protected files. When encryption is impractical or unavailable transmit over regular email channels.

4.3.4 UNENCRYPTED FILES

Unencrypted files containing CUI/SBU information shall ***NEVER*** be stored or transmitted using commercial file sharing systems (e.g., Dropbox).

4.3.5 PUBLIC WEBSITES

CUI/SBU information should not be posted to public websites.

a. SSI may be posted on approved government-controlled or –sponsored encrypted or otherwise protected portals, such as the Homeland Security Information Network (HSIN), USCG HomePort, or TSA's WebBoards. Such posting shall be in accordance with guidance published or approved by the TSA SSI Office and appropriate IT security offices.

4.4 RELEASE TO ELIGIBLE STAKEHOLDERS

CoSSaR may disseminate CUI/SBU information to its employees and subcontractors who have a need for the information to complete work assigned in connection with CoSSaR projects.

CoSSaR seeks to provide its CUI/SBU information-designated analytic products the widest distribution among Puget Sound area stakeholders with a legitimate "need to know".

a. The CoSSaR Program Manager will seek permission from its DHS sponsor team to release reports containing CUI/SBU information to each individual stakeholder requesting the information.

b. The CoSSaR Project Manager will also comply with University procedures for the release of CUI/SBU information by submitting a University Access Request Form to release CUI/SBU information to regional stakeholders.

C. The CoSSaR Project Manager will maintain a log recording the release of all CoSSaR products and reports containing CUI/SBU information to third parties.

4.5 DESTRUCTION

Hard copy CUI/SBU materials will be destroyed by shredding, burning, pulping, or pulverizing, sufficient to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

Electronic storage media shall be sanitized appropriately by overwriting or degaussing. After destruction, materials may be disposed of with normal waste.

Paper products containing CUI/SBU materials will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

4.6 INCIDENT REPORTING

The loss, compromise, suspected compromise, or unauthorized disclosure of CUI/SBU information will be reported to the CoSSaR program's DHS sponsor team and the University of Washington Office of Sponsored Programs within one business day of the discovery of the incident.

Incidents on UW IT systems will also be reported to the University Facility Security Officer at 206-543-1315 or uwfso@uw.edu via the system's Information Technology Manager (http://ciso.washington.edu/report/). Coordinate reporting through the HCDE IT Manager for incidents on the HCDE server or the APL IT Manager for incidents on APL-hosted servers.

Suspicious or inappropriate requests for CUI/SBU information by any means (e.g., email or verbally) shall be reported to the DHS sponsor team via the CoSSaR Program Manager and the UW Office of Sponsored Programs.

If the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned ongoing operation, additional notifications to appropriate DHS management personnel will be made without delay.

In the event of an unauthorized disclosure, CoSSaR will request an inquiry by the University Facility Security Officer to determine the cause and effect of the incident and suggested corrective actions to prevent recurrence.

5 General Guidance, “FOR OFFICIAL USE ONLY”

The following matrix has been compiled to assist CoSSaR personnel to recognize information that requires control as “For Official Use Only”. ***This is an abridged list*** containing the most likely topics CoSSaR researchers are expected to encounter in the conduct of their research. ***Appendix A contains a list of all topics provided by DHS in Management Directive 11042.1.***

Table 3: FOUO General Guidance		
For Official Use Only – 5 USC 552 (FOIA and Privacy Act)		
Topic	**Marking**	**Remarks**
FOIA (5 USC 552) Exemption 1: Properly classified information	As Marked	CoSSaR will not receive, process, or handle classified material.
FOIA (5 USC 552) Exemption 2: Records related to the internal personnel rules and practices of an agency.	FOUO	
FOIA (5 USC 552) Exemption 3: Information that has been specifically exempted from disclosure by statute.	FOUO	
FOIA (5 USC 552) Exemption 4: Trade Secrets (narrowly defined)	FOUO	
FOIA (5 USC 552) Exemption 5: Inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.	FOUO	
FOIA (5 USC 552) Exemption 6: Personnel, medical, and similar files	FOUO	

FOIA (5 USC 552) Exemption 7: Law enforcement information	FOUO-LES	See Law Enforcement Sensitive Matrix for further guidance
FOIA (5 USC 552) Exemption 8: Matters/information for regulators or supervisors of financial institutions	FOUO	
FOIA (5 USC 552) Exemption 9: Geological information and data, including maps, concerning wells	FOUO	
Privacy Act (5 USC 552a) § (j)(2): Material reporting investigative efforts pertaining to the enforcement of criminal law, including efforts to prevent, control, or reduce crime or to apprehend criminals.	FOUO-LES	See Law Enforcement Sensitive Matrix for further guidance
International and domestic information protected by treaty, statute, regulation, or other agreement.	FOUO	
Information that could result in physical risk to personnel.	FOUO	
System security data revealing the security posture of a system.	FOUO	For example: threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, etc…
Information that reveals security vulnerabilities, whether to persons, systems, or facilities.	SSI	See Sensitive Security Information Matrix for further guidance

6 General Guidance, “Law Enforcement Sensitive”

The following matrix has been compiled to assist CoSSaR personnel to recognize information that requires control as “Law Enforcement Sensitive”. The list contains abridged descriptions. Appendix B contains the full descriptions of Law Enforcement Sensitive exclusions to the FOIA as delineated by the US Department of Justice.

Table 4: LES General Guidance		
Law Enforcement Sensitive – Exemption 7 of FOIA (5 USC 552)		
Topic	**Marking**	**Remarks**
Information that could reasonably be expected to interfere with enforcement proceedings	FOUO-LES	
Information that would deprive a person of a right to a fair trial or an impartial adjudication	FOUO-LES	
Information that could reasonably be expected to constitute an unwarranted invasion of personal privacy	FOUO-LES	
Information that could reasonably be expected to disclose the identity of a confidential source	FOUO-LES	Including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation,

		information furnished by a confidential source
Information that would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law	FOUO-LES	
Information that could reasonably be expected to endanger the life or physical safety of any individual	FOUO-LES	

7 General Guidance, “Sensitive Security Information”

The following matrix has been compiled to assist CoSSaR personnel to recognize information that requires control as “Sensitive Security Information” as delineated in 49 US Code of Federal Regulations (CFR) §1520.5.

(From https://www.tsa.gov/sites/default/files/assets/pdf/ssi/16_categories_ssi.pdf)

(See also: https://www.law.cornell.edu/cfr/text/49/1520.5)

Table 5: SSI General Guidance		
Sensitive Security Information – 49 CFR (Code of Federal Regulations) §1520.5		
Topic	**Marking**	**Remarks**
Security Programs and Contingency Plans	SSI	Includes amendments, comments, guidance regarding: i. Domestic aircraft operator, airport, foreign a/c, FBO, or IAC security program or contingency plan ii. Vessel, maritime facility, port security plan [maritime only] iii. National or area security plan [maritime only] iv. Security incident response plan [maritime only]
Security Directives (SDs) or orders	SSI	i. Issued by TSA for domestic aircraft or airport operators ii. Issued by Coast Guard [maritime only] iii. Related comments, guidance
Info Circulars or notices issued by DHS or DOT regarding aviation or maritime threats	SSI	i. Info Circulars (ICs) issued by TSA ii. Navigation or Vessel Inspection

		Circulars (NAVICs) issued by USCG [maritime only]
Performance specifications, test objects, and test procedures	SSI	i. Detection devices used by Fed Government for aviation or maritime security [devices] ii. Security communications equipment used for aviation or maritime [comm. equipment only]
Vulnerability assessments directed, created, held, funded, approved by, or provided to, DOT or DHS	SSI	
Security Inspection or investigation information	SSI	i. Details revealing an aviation or maritime vulnerability (less than one year old), including airport and aircraft name and violation description; identity of investigating Federal employee ii. (After one year) specific gate or airport location; (within one year) airport violation summaries [release airport and a/c name and violation description after one year]
Threat information against transportation held by Government	SSI	

Security measures: specific details of aviation or maritime security measures	SSI	i. Measures recommended by the Government ii. Procedures and #s of Federal Air Marshals (FAMs) or USCG security personnel iii. Procedures, or aggregated #s by aircraft operator, of Federal Flight Deck Officers (FFDOs) iv. Armed security officer procedures [Armed Security Officer Prog. for DCA general aviation]
Security screening info (aviation or maritime)	SSI	i. Procedures, incl. comments, guidance, and selection criteria, for screening persons, carry-on or checked baggage, U.S. mail, and stores [CAPPS criteria] ii. Info and sources of info of screening systems [actual No Fly lists] iii. Detailed locations of particular screening methods or equipment [requires determination] iv. Any security screener tests and scores [written, procedural, computer-based tests] v. Performance or testing data from security equip. or screening systems [operational tests] vi. Any electronic image on

		screening equip. monitors, incl. TIPS images/descriptions
Security training materials created for aviation or maritime security training purposes	SSI	
Identifying info of certain transportation security personnel	SSI	i. Lists of names or identifying info: [lists, not individual names] 1. Having unescorted access to secure area of airport or maritime facility 2. Security screeners aggregated by airport 3. USCG personnel conducting vulnerability assessments, security boardings, other operations 4. FAMS ii. FFDOs [individual names, not just lists]
Critical aviation or maritime infrastructure asset info	SSI	i. Prepared by DHS or DOT ii. Prepared by State or Local government and submitted to DHS or DOT
Confidential business information related to aviation or maritime security	SSI	i. Solicited or unsolicited proposals ii. Trade secret info obtained by DHS and DOT iii. Commercial or financial info, if not otherwise customarily disclosed

Research and Development info	SSI	Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.
Other	SSI	Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

APPENDIX A: Information Controlled as “For Official Use Only”

1. Information that is exempt from release under FOIA (5 U.S.C. 552)
http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-exemptions.pdf

a. Exemption 1: Protects properly classified information.

b. Exemption 2: Protects records that are “related solely to the internal personnel rules and practices of an agency.”

c. Exemption 3: Protects information that has been “specifically exempted from disclosure by statute.”

d. Exemption 4: Protects trade secrets (narrowly defined).

e. Exemption 5: Protects “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.”

f. Exemption 6: Protects information in personnel and medical files and similar files when disclosure would constitute a clearly unwarranted invasion of personal privacy.

g. Exemption 7: Protects six different types of law enforcement information: On-going proceedings; Personal Privacy; Confidential sources; Techniques and procedures. (See Law Enforcement Sensitive section below).

h. Exemption 8: Protects matters contained in or related to examination, operating, or condition reports prepared by or for regulators or supervisors of financial institutions.

i. Exemption 9: Protects geological information and data, including maps, concerning wells.

2. Information that is exempt from release under Privacy Act (5 U.S.C. 552a)
http://www.fbi.gov/foia/privacy-exemptions

a. Information compiled in reasonable anticipation of a civil action proceeding.

b. Material reporting investigative efforts pertaining to the enforcement of criminal law, including efforts to prevent, control, or reduce crime or to apprehend criminals.

c. Information that is currently and properly classified pursuant to an executive order in the interest of the national defense or foreign policy—for example, information involving intelligence sources or methods.

d. Investigative material compiled for law enforcement purposes, other than criminal, which did not result in the loss of a right, benefit, or privilege under federal programs or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence.

e. Material maintained in connection with providing protective services to the U.S. President or any other individual pursuant to the authority of Title 18, U. S. Code, Section 3056.

f. Required by statute to be maintained and used solely as statistical records.

g. Investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence.

h. Testing or examination material used to determine individual qualifications for appointment or promotion in federal government service—the release of which would compromise the testing or examination process.

i. Material used to determine the potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

3. Information within the international and domestic banking and financial communities protected by statute, treaty or law.

4. Other international and domestic information protected by treaty, statute, regulation, or other agreement.

5. Information that could be sold for profit.

6. Information that could result in physical risk to personnel.

7. DHS Information Technology (IT) internal systems data.

8. System security data revealing the security posture of a system. For example threat assessments, system security plans, risk management plans, etc…

9. Information that reveals security vulnerabilities, whether to persons, systems, or facilities.

10. Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten national security.

11. Overly revealing information of developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.

APPENDIX B: Law Enforcement Sensitive (LES) Information

http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/exemption7_0.pdf

Exemption 7 of the Freedom of Information Act protects from disclosure "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information that

(A) could reasonably be expected to interfere with enforcement proceedings,

(B) would deprive a person of a right to a fair trial or an impartial adjudication,

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual."

DEFINITIONS

Access. The ability and opportunity to obtain knowledge of classified information.

Classified National Security Information. Information that has been determined pursuant to E.O. 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Also, known as classified information.

Compilation. An aggregation of pre-existing unclassified items of information. Compilations of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification pursuant to E.O. 13526 and is not otherwise revealed by the individual information. Classification by compilation must meet the same standards and criteria as other original classification actions.

Document. Recorded information regardless of the nature of the medium or the method or circumstances of recording.

For Official Use Only (FOUO). The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interests. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 13526, "Classified National Security Information", or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Information. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by produced by or for, or is under the control of the United States Government.

Law Enforcement Sensitive (LES). "Law Enforcement Sensitive" is a marking sometimes applied, in addition to the marking "FOR OFFICIAL USE ONLY," by the Department of Justice and other activities in the law enforcement community, including those within the Department of Defense. It denotes that the information was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests.

Lawful Request. Any formal request for information or records that is made under the auspices of existing statute or regulation, for example, information or records requested under the Freedom of Information Act (FOIA).

Need-to-know. A determination within the executive branch in accordance with directives issued pursuant to E.O. 13526 that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Sensitive Security Information (SSI). As defined in 49 C.F.R. Section 1520.5, information obtained or developed in the conduct of security activities, including research and development, the disclosure of which DHS/TSA has determined would (1) constitute an unwarranted invasion of privacy (including , but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

Unclassified. Information not meeting criteria for classification set forth in Executive Order 13526.